CLAIMS

Please amend the presently pending claims as follows:

Claims 1-35 (Cancelled)

36. (Previously Presented) A method for generating shared keys comprising:

    providing a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters that comprises a first public key for the first peer;

    generating a second public key by the second peer with at least one parameter of the plurality of first parameters and a first private key of the second peer;

    providing the generated second public key from the second peer to the first peer;

    generating a first shared secret key for the second peer with the first public key of the first certificate; and

    generating a second shared secret key for the first peer with the second public key from the second peer and a private key of the first peer.

37. (Previously Presented) The method of claim 36 and further comprising providing a second certificate from the second peer to the first peer, the second certificate comprising a plurality of second parameters.

38. (Previously Presented) The method of claim 37 wherein generating the second shared secret key for the first peer with the second public key from the second peer and a private key of the first peer further comprises generating the second shared secret key for the first peer with the second public key from the second peer, the private key of the first peer and at least one of the plurality of second parameters.

39. (Previously Presented)   The method of claim 36 wherein the first public key of the first certificate is received from a third party certificate authority.

40. (Cancelled)   The method of claim 36 wherein generating a first shared secret key for the second peer with the first public key of the first certificate is carried out independently of any public key generated by the first peer and the second peer.

41. (Previously Presented)   The method of claim 36 wherein the plurality of first parameters of the first certificate comprises at least one prime number and at least one generator in addition to the first public key of the first certificate.

42. (Previously Presented)   The method of claim 37 wherein the plurality of second parameters of the second certificate comprises at least one prime number, at least one generator and a public key of the second certificate that is received from a third party certificate authority.

43. (Previously Presented)   The method of claim 42 and wherein the generating a second shared secret key for the first peer with the second public key from the second peer and a private key of the first peer is carried out without employing either the first public key of the first certificate or the public key of the second certificate.

44. (Previously Presented)   The method of claim 37 wherein both the first certificate including the plurality of first parameters and the second certificate including the plurality of second parameters are generated independently of the first peer and the second peer.

45. (Previously Presented)   The method of claim 37 wherein both the first certificate and the second certificate comprise Digital Signature Algorithm (DSA) type certificates.

46. (Previously Presented)   The method of claim 37 wherein the plurality of first parameters and the plurality of second parameters comprise digital signature standard parameters.

47. (Previously Presented)   The method of claim 37 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.

48. (Previously Presented)   The method of claim 36 wherein the first peer and the second peer communicate over a network.

49. (Previously Presented)   The method of claim 48 wherein the network comprises at least one of a wireless network or a Bluetooth network.

50. (Previously Presented)   The method of claim 36 wherein the first public key of the first certificate is a variable used in the step of generating the first shared key.

51. (Previously Presented) A system comprising:

    a processor; and

    a memory coupled to the processor, the memory containing program code that, when executed by the processor, causes the processor to:

        provide a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters that comprises a first public key for the first peer;

        generate a second public key by the second peer with at least one parameter of the plurality of first parameters and a first private key of the second peer;

        provide a second certificate and the second public key from the second peer to the first peer, the second certificate comprising a plurality of second parameters;

generate a first shared secret key for the second peer with the first public key of the first certificate; and

generate a second shared secret key for the first peer with the second public key from the second peer, a private key from of first peer and at least one of the plurality of second parameters.

52. (Previously Presented)   The system of claim 51 wherein both the first certificate including the plurality of first parameters and the second certificate including the plurality of second parameters are generated independently of the first peer and the second peer.

53. (Previously Presented)   The system of claim 51 wherein both the first certificate and the second certificate comprise Digital Signature Algorithm (DSA) type certificates.

54. (Previously Presented)   The system of claim 51 wherein the plurality of first parameters and the plurality of second parameters comprise digital signature standard parameters.

55. (Previously Presented)   The system of claim 51 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.

56. (Previously Presented)   The system of claim 51 wherein the first peer and the second peer communicate over a network that comprises at least one of a wireless network or a Bluetooth network.

57. (Previously Presented)   A computer storage medium including data that, when accessed by a computer, causes the computer to perform operations comprising:

providing a first certificate from a first peer to a second peer, the first certificate including

a plurality of first parameters that comprises a first public key for the first peer;

generating a second public key by the second peer with at least one parameter of the

plurality of first parameters and a first private key of the second peer;

providing a second certificate and the second public key from the second peer to the first peer, the second certificate comprising a plurality of second parameters;

generating a first shared secret key for the second peer with the first public key of the first certificate; and

generating a second shared secret key for the first peer with the second public key from the second peer, a private key from of first peer and at least one of the plurality of second parameters.

58. (Previously Presented)   The computer storage medium of claim 57 wherein both the first certificate including the plurality of first parameters and the second certificate including the plurality of second parameters are generated independently of the first peer and the second peer.

59. (Previously Presented)   The computer storage medium of claim 57 wherein both the first certificate and the second certificate comprise Digital Signature Algorithm (DSA) type certificates.

60. (Previously Presented)   The computer storage medium of claim 57 wherein the plurality of first parameters and the plurality of second parameters comprise digital signature standard parameters.

61. (Previously Presented)   The computer storage medium of claim 57 wherein the first and second certificates are sent to the second and first peers, respectively, over a wireless network.

62. (Previously Presented)   The computer storage medium of claim 57 wherein the first peer and the second peer communicate over a network that comprises at least one of a wireless network or a Bluetooth network.

63. (New) A method for generating shared keys comprising:

> providing a first certificate from a first peer to a second peer, the first certificate including a plurality of first parameters that comprises a first public key for the first peer;

> generating a second public key by the second peer with at least one parameter of the plurality of first parameters and a first private key of the second peer;

> providing the generated second public key from the second peer to the first peer;

> generating a first shared secret key for the second peer with the first public key of the first certificate; and

> generating a second shared secret key for the first peer with the second public key from the second peer and a private key of the first peer,

> wherein generating the first shared secret key for the second peer with the first public key of the first certificate is carried out independently of any public key generated by the first peer and the second peer.